CLAIMS

What is Claimed is:

1. A method comprising:

stalling a request; and

determining whether the request is suspicious,

wherein upon a determination that the request is suspicious, determining whether malicious code activity is detected based upon the request.

2. The method of Claim 1, further comprising:

wherein upon a determination that malicious code activity is detected, generating a notification that malicious code activity is detected; and

implementing one or more protective actions.

3. A method comprising:

intercepting a request on a host computer system;

stalling the request; and

determining whether the request is suspicious,

wherein upon a determination that the request is suspicious, adding a request entry representative of the request to a request database, and

determining whether malicious code activity is detected on the host computer system based upon the request entry.

4. The method of Claim 3, further comprising:

wherein upon a determination that the request is not suspicious, releasing the request.

5. The method of Claim 3, further comprising:

wherein upon a determination that malicious code activity is detected on the host computer system, generating a notification that malicious code activity is detected on the host computer system; and

implementing one or more protective actions.

6. The method of Claim 3, further comprising:

wherein upon a determination that malicious code activity is not detected on the host computer system, releasing the request.

7. The method of Claim 3, wherein the determining whether malicious code activity is detected on the host computer system based upon the request entry further comprises:

generating a counter value associated with the request entry; and

determining whether the counter value meets a counter value threshold,

wherein upon a determination that the counter value does not meet the counter value threshold, determining that malicious code activity is not detected on the host computer system, and

wherein upon a determination that the counter value meets the counter value threshold, determining that malicious code activity is detected on the host computer system.

8. The method of Claim 3, wherein the implementing one or more protective actions comprises:

terminating the request.

9. The method of Claim 3, wherein the request is an HTTP GET request.

10. The method of Claim 3, wherein the intercepting a request on a host computer system utilizes a local proxy mechanism.

11. The method of Claim 3, wherein the intercepting a request on a host computer system occurs at the application level.

12. A malicious code detection device comprising:

an intercept module;

an analyzer module coupled to the intercept module;

a request database coupled to the analyzer module; and

a standards list coupled to the analyzer module.

13. The malicious code detection device of Claim 12, further comprising:

an inclusion profile list coupled to the analyzer module.

14. The malicious code detection device of Claim 12, further comprising:

an exclusion profile list coupled to the analyzer module.

15. The malicious code detection device of Claim 12, further comprising a memory area coupled to the intercept module and the analyzer module.

16. The malicious code detection device of Claim 12, wherein the intercept module includes an interception mechanism for intercepting a request.

17. A computer program product comprising a computer-readable medium containing computer program code for a method comprising:

stalling a request; and

determining whether the request is suspicious,

wherein upon a determination that the request is suspicious, determining whether malicious code activity is detected based upon the request.

18. The computer program product of Claim 17, the method further comprising:

wherein upon a determination that malicious code activity is detected, generating a notification that malicious code activity is detected; and

implementing one or more protective actions.

19. A computer program product comprising a computer-readable medium containing computer program code for a method comprising:

intercepting a request on a host computer system;

stalling the request; and

determining whether the request is suspicious,

wherein upon a determination that the request is suspicious, adding a request entry representative of the request to a request database, and

determining whether malicious code activity is detected on the host computer system based upon the request entry.

20. The computer program product of Claim 19, the method further comprising:

wherein upon a determination that malicious code activity is detected on the host computer system, generating a notification that malicious code activity is detected on the host computer system; and

implementing one or more protective actions.